Appl. No. 09/587,932
Amdt. dated December 27, 2004
Amendment under 37 CFR 1.116 Expedited Procedure
Examining Group

PATENT

REMARKS/ARGUMENTS

The office action initially rejected claims 1-5 and 7-9 under 35 U.S.C. §102 as being anticipated by Chan (U.S. Pat. 6,609,202). Furthermore, claims 10-23 were rejected under 35 U.S.C. §103 in view of Chan. Claim 6 was rejected under 35 USC §103 as unpatentable over the combination of Chan and Matthews (US Pub. No. 20030005292A1).

Section 102 Issues

Claim 1 was rejected as being anticipated by Chan. This rejection is respectfully traversed. The Chan reference is directed at a system for distributing computer code to a plurality of units (See Chan Abstract). However, claim 1 of Applicant's application is directed at delivering encrypted streams of data to the same destination device. The office action rejected claim 1 by citing portions of column 13 in Chan. However, that portion of Chan refers to sending information to two _different_ destination devices. For the examiner's convenience, claim 11 from the Chan reference is quoted below. This passage is the passage relied upon in the office action:

Claim 11 from the Chan reference that was relied upon in the office action

A method for delivering displayable data to a plurality of processing units, each of said processing units being located in a separate remote site and connected to an output unit, said method comprising:

providing a first and a second set of digital data, said first set of digital data being encrypted at a first level and comprising a content portion and an identification label, said content portion being displayable on said output unit, said second set of digital data being displayable on said output unit and related to said first set of digital data;

distributing said first set of digital data to each of said plurality of processing units;

Appl. No. 09/587,932
Amdt. dated December 27, 2004
Amendment under 37 CFR 1.116 Expedited Procedure
Examining Group

PATENT

receiving said identification label from at least a first and a second one of said processing units;

after receiving said identification label from said first processing unit:

generating a first encrypted digital data by encrypting said second set of digital data at a second level using a first key, and

delivering said first encrypted digital data to said first processing unit; and after receiving said identification label from said second processing unit:

generating a second encrypted digital data by encrypting said second set of digital data at a level different than said first level using a second key, and

delivering to said second processing unit said second encrypted digital data.

Portions of the cited passage have been emphasized herein to highlight the fact that the encrypted digital data is not being delivered to the same destination device for decryption, as recited in claim 1 of applicant's application. Rather, the Chan reference states that its first encrypted digital data stream is delivered to a first processing unit while its second encrypted digital data stream is delivered to a second processing unit. Furthermore, the preamble of Chan notes that the processing units are each located separately. Thus, it is clear that Chan does not teach each of the elements of claim 1, since it does not teach sending the first and second data streams to the same destination device for decryption. Consequently, claim 1 is believed to be in condition for allowance. Since claims 2-5 and 7-9 depend from claim 1, they are allowable for the same reasons as claim 1.

However, it is noted that the office action is incorrect in rejecting the dependent claims for additional reasons. For example, claim 7 recites the additional element of "storing a plurality of decryption algorithms at said set-top box." The office action cited the following

Appl. No. 09/587,932
Amdt. dated December 27, 2004
Amendment under 37 CFR 1.116 Expedited Procedure
Examining Group

PATENT

section from Chan, namely Col. 4, lines 35-45 and col. 10, lines 29-40. Those sections read as follows:

> "The key used for encrypting and decrypting the encrypted data
> could be different for each processing and communication session
> described above. Thus, it is more difficult for unauthorized persons
> to obtain the decryption key to decrypt the encrypted data. Even
> assuming that a few decryption keys are inadvertently disclosed to
> unauthorized persons, only a few pieces of information is
> compromised. This is different from the system disclosed in the
> prior art, where inadvertent disclosure of a single decryption key
> may compromise vast amount of information. "

> "Secure processor 420 contains an internal processor 428 and
> RAM 430 that together perform, among other tasks, authentication,
> decryption, and/or decompression. The central station 446 may
> also send instructions (in encrypted form) to internal processor 428
> for execution. These instructions may be part of a decryption
> algorithm for decryption a particular piece of encrypted data sent
> by central station 446 to secure processor 420. The instruction set
> of internal processor 428 is preferably hidden from the general
> public. As a result, it is difficult for an unauthorized person to
> execute these instructions, even if the decryption key is
> inadvertently discovered by such person."

There is clearly no discussion of storing a plurality of decryption algorithms at a set-top box in these cited passages. Therefore, this claim is clearly not anticipated by Chan.

Appl. No. 09/587,932
Amdt. dated December 27, 2004
Amendment under 37 CFR 1.116 Expedited Procedure
Examining Group

PATENT

Section 103 Issues

Claim 10 has been amended by including the concept from claim 12 into claim 10. While the office action cites Chan at column 4, lines 26-34 and column 11, lines 62-67 in rejecting claim 12 (which has now been incorporated into claim 10), there is clearly no discussion in these sections of a memory. Furthermore, there is no discussion of a memory that stores a plurality of encryption algorithms. Thus, it is believed that claim 10 as amended is in condition for allowance. Since the amendment merely incorporated an element from a dependent claim, it is believed that the amendment does not necessitate a new search by the examiner. Claims 11 and 13 depend from claim 10. Therefore, they are believed to be in condition for allowance for at least the same reasons that claim 10 is allowable.

Similar to claim 10, claim 14 has been amended to recite that a memory is used to store the first set of decryption data corresponding to a first level of encryption and said second set of decryption data corresponding to said second level of encryption. Thus, claim 14 is not obvious under §103 in view of the Chan reference. Claims 15-18 which depend from claim 14 are allowable for the same reasons that claim 14 is allowable.

Claims 19-22 are cancelled without prejudice or disclaimer.

Claim 23 recites "storing a plurality of decryption algorithms in said set-top box." As noted above, the Chan reference does not contemplate storage of a plurality of decryption algorithms. Therefore, for at least this reason, claim 23 is allowable. Furthermore, the applicant respectfully traverses the assertion that the client secure processor in the Chan reference is a set-top box. For at least these reasons, claim 23 is believed to be allowable.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.
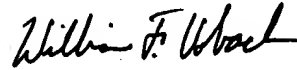
Appl. No. 09/587,932
Amdt. dated December 27, 2004
Amendment under 37 CFR 1.116 Expedited Procedure
Examining Group

PATENT

Respectfully submitted,

William F. Vobach
Reg. No. 39,411

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300
WFV:klb
60386272 v1